36th Annual Forensic Mental Health Association of California Conference

## HIPAA, HITECH, SB 541 and AB 211:

*Everything You Need to Know About the Increasing Federal and State Enforcement of Confidentiality Rights*

Friday, March 25, 2011
10:30 a.m. – 12 noon

Presenter: Linda J. Garrett, JD
Risk Management Services
707-792-4980
lindagarrett.risk@comcast.net

## Why worry about confidentiality of medical information?

- Recently a researcher in Southern California pled guilty to 4 misdemeanor counts of inappropriately accessing patient information (he "peeked" at celebrity and other high profile patient records).
- He was sentenced to 4 months in federal prison!

## Examples of recent State fines under new State laws

- Kaweah Manor Convalescent Hospital (Visalia) - $125,000 fine after unauthorized access and use of five patients' info by one employee
- San Joaquin Community Hospital (Bakersfield) – fined $25,000 after it failed to prevent unauthorized access of three patients' info by two employees.

## Examples of State Fines - continued

- Children's Hospital of Orange - $25,000 failed to prevent access to one chart by one employee
- Delano Regional Medical Center - $60,000 after unauthorized access and disclosure of one patient's info by one employee on three occasions

## State Fines -continued

- Community Hospital of San Bernardino - $250,000 after finding that it failed to prevent unauthorized access of 204 patients' medical information by one employee; another $75,000 fine after facility failed to prevent unauthorized access of three patients' medical information by one employee (max of $25,000 for each file accessed)

## State fines -continued

- Kern Medical Center (Bakersfield) - $60,000 after unauthorized access and disclosure of one patient's info by two employees on three occasions; $250,000 after it failed to prevent the theft of 596 patients' medical information
- Oroville Hospital - $42,500 after it failed to prevent unauthorized disclosure of one patient's info by one employee on two occasions ($25,000 for the 1st violation with $17,500 for each subsequent violation)

## State fines -continued

- Pacific Hospital of Long Beach - $225,000 fine after facility failed to prevent unauthorized access and use of nine patients' medical info by one employee

## State fines – more examples

- Enloe Medical Center (Chico) - $130,000 after it failed to prevent unauthorized access of one patient's chart by seven employees ($25,000 plus 6 x $17,500)
- Rideout Memorial Hospital (Marysville) - $100,000 fine after it failed to prevent access of 33 patients' medical information by 17 employees
- Ronald Reagan UCLA Medical Center - $95,000 after it failed to prevent access to one chart by four employees

## Why now?

- New laws require mandatory self-reporting to both the State and Federal Government by health care facilities (State), and "covered entities" and "business associates" (Fed)
- *(Also, some have noted that the enthusiastic enforcement of financial penalties by the State appears linked to the its need to resolve its budget crisis!)*

9

## Federal laws

- HIPAA – effective April 14, 2003 "covered entities" had a duty to do two things if there was a breach of privacy:
  1. Mitigate the harm
  1. Sanction the wrong-doer

10

## (Are you a "Covered Entity"?)

- Are you a health care provider that bills electronically using standardized transactions and code sets?
- Are you a health insurance plan?
- Are you creating protected health information ("PHI") or merely receiving and collecting it from other CE's?

11

## (Not a covered entity?)

- Even if you aren't a CE (for example correctional care providers who don't bill electronically for individual services, or Court employee hired to evaluate inmates re: insanity defense or competence to stand trial) it's good to know about HIPAA since you'll deal with CE's often in your work
- (And, even though HIPAA/HITECH reporting might not apply, State law might!)

12

## (Are you a Business Associate?)

- When a "covered entity" contracts with a person/entity to help it with its own operations and the work requires access to, or use of, "protected health information" (PHI) then a Business Associate Agreement is required
- BA Examples: a company that shreds old records, CPA who helps prepare for audit, IT person who converts to electronic health record ("EHR"), external peer reviewer, malpractice attorney

13

## HIPAA – "mitigating the harm" if there was a breach

- Nothing in HIPAA explained what mitigation had to entail
- Therefore, unless someone's name, birth-date and social security number got into the hands of a criminal, we usually didn't notify the patient

14

## HITECH Act

- ARRA/HITECH Act – signed into law on February 17, 2009 (American Reinvestment and Recovery Act/Health Information Technology for Economic and Clinical Health Act)
- Regulations/Notice of Proposed Rulemaking published August 24, 2009
- HIPAA privacy breaches occurring on or after September 23, 2009 must be reported to DHHS (immediately if 500+ and annually if small breach); patient must be notified without reasonable delay (but no longer than 60 days)

## 3 Exceptions
The term "breach" does not include:

1. Mistaken access by employee
2. Mistaken disclosure by one employee to another
3. Near miss

16

## Plus, there is a "harm threshold"

- Regulations published in Fed. Register in August 2009 surprised many with addition of "threshold of harm" requirement (meaning you didn't have to report to DHHS or notify the patient unless there was a risk of substantial reputational, financial or other harm)
- August 2010 – final rules submitted in May by Secretary of DHHS were withdrawn at request of Obama Administration after outpouring of criticism; but, they remain in effect until new rule is issued!

17

## "Risk of harm" assessment

- Covered entity needs to do assessment in the case of every potential reportable breach to determine whether it poses a significant risk of harm to the patient
- This risk assessment should be documented and retained for at least 6 years

## State Laws SB 541 and AB 211

- SB 541 – beginning January 1, 2009, state law required health care facilities licensed under H&S Code 1250 (and other sections) to report ALL breaches to the CA Department of Public Health
- Facilities include 24 hour care hospitals, acute psych hospitals, psychiatric health facilities, home health agencies, hospices, and primary care and specialty clinics operated by non-profit corporations AND correctional care "inpatient" facilities (see next slide)

## H&S Code 1250 also includes correction care treatment centers

(j) (1) "Correctional treatment center" means a health facility operated by the Department of Corrections and Rehabilitation, the Department of Corrections and Rehabilitation, Division of Juvenile Facilities, or a county, city, or city and county law enforcement agency that, as determined by the state department, provides inpatient health services to that portion of the inmate population who do not require a general acute care level of basic services. This definition shall not apply to those areas of a law enforcement facility that houses inmates or wards that may be receiving outpatient services and are housed separately for reasons of improved access to health care, security, and protection. The health services provided by a correctional treatment center shall include, but are not limited to, all of the following basic services: physician and surgeon, psychiatrist, psychologist, nursing, pharmacy, and dietary. A correctional treatment center may provide the following services: laboratory, radiology, perinatal, and any other services approved by the state department.

20

(2) Outpatient surgical care with anesthesia may be provided, if the correctional treatment center meets the same requirements as a surgical clinic licensed pursuant to Section 1204, with the exception of the requirement that patients remain less than 24 hours.

(3) Correctional treatment centers shall maintain written service agreements with general acute care hospitals to provide for those inmate physical health needs that cannot be met by the correctional treatment center.

(4) Physician and surgeon services shall be readily available in a correctional treatment center on a 24-hour basis.

(5) It is not the intent of the Legislature to have a correctional treatment center supplant the general acute care hospitals at the California Medical Facility, the California Men's Colony, and the California Institution for Men. This subdivision shall not be construed to prohibit the Department of Corrections and Rehabilitation from obtaining a correctional treatment center license at these sites.

21

## State breach reporting

- Requires report to CDPH within 5 business days
- CDPH then notifies Cal OHII and Cal OHII notifies licensing boards of any involved licensed employees of facilities so they may discipline their licensee's
- CDPH has power to levy fines up to $25,000 (and up to $250K if there was an intentional breach for financial gain) -- as well as other penalties

## AB 211

- Makes breach of privacy that results in economic loss or personal injury punishable as a misdemeanor (Civil Code 56.36)
- Applies to health care providers AND to "any person or entity other than a licensed health care professional, who knowingly and willfully obtains, discloses, or uses medical information in violation of (the Confidentiality of Medical Information Act)."

23

## CHA letter to CDPH re: confusion caused by federal/state reporting schemes

- December 13, 2010 letter in response to proposed regulations re: medical information breaches described in H&S Code 1280.15
- Respectfully requests that CA law be crafted to harmonize state efforts with federal law and regulation to reduce confusion, conflict, and the need for costly pre-emption evaluation in the event of a breach

## Letter -continued

- Notes that CA law does not allow time to substantiate a breach before it must be reported
- Notes that CA law does not include any provision re: evaluation of patient "harm"
- Notes no time frame for CDPH to respond to reports so many months, up to a year, may pass before investigation or levying of fines and hearing of appeals (reported cases thus appear to be "open" indefinitely)

## Letter -continued

- Notes that CDPH and Office of Health Information Integrity (OHII), which is tasked with AB 211 investigations of individuals, are not coordinated in their follow-up, leading to duplicate investigations and costs (with no individual citations to date)
- Notes that despite all efforts, rogue employees end up costing hospitals thousands of dollars under strict liability approach

## Letter -continued

- No allowances for non-malicious erroneous disclosures (internal faxing errors)
- Punitive atmosphere (so far fines have always been the maximum $25,000 regardless of the nature of the breach)

## AB 211, SB 541 and HITECH Act: Summary of State and Federal penalties

State – up to $25,000 per breach; if used for financial gain, up to $250,000 administrative fine or civil penalty

Feds

HIPAA (April 14, 2003) – complaint driven: not more than $100 for each violation subject to $25,000 calendar-year cap for identical violations

HITECH Act (Feb. 18, 2010) – now more aggressive and punitive strategy: 4 tiers, w/maximum of $1.5 million for all violations of identical provision/calendar year

## Penalties - continued

- Other penalties
  - State
    - Health and Safety Code section 130205

      ...the director may send a recommendation for further investigation of, or discipline for, a potential violation of this division to the licensee's relevant licensing authority. ... The licensing authority...may take action for further investigation or discipline of the licensee.

## Penalties - continued

Other Penalties

- Federal
  - Disclosure to another person: up to $50,000 fine and up to one year in prison
  - False pretenses: up to $100,000 and 5 years
  - With intent to sell: up to $250,000 and 10 years

30

## Reaction to fines and penalties

- Dec. 4, 2010 article: "California hospitals and nursing homes take note: the California Department of Public Health (CDPH) takes data breaches seriously. Since June of this year (2010) CDPH has imposed nearly $1.5 million in fines affecting 12 California health facilities."

## Criticism is growing

- Some believe the punitive atmosphere will result in under-reporting which defeats some of the quality improvement purposes of the reporting framework
- Some see actions of CDPH as "balancing budget deficits on the backs of the hospitals"

## One more thing about penalties . . . Civil Code 56.36 (e) provides:

- (e) (1) The civil penalty pursuant to subdivision (c) shall be assessed and recovered in a civil action brought in the name of the people of the State of California in any court of competent jurisdiction by any of the following:
  - (A) The Attorney General.
  - (B) Any district attorney.
  - (C) Any county counsel authorized by agreement with the district attorney in actions involving violation of a county ordinance.
  - (D) Any city attorney of a city.
  - (E) Any city attorney of a city and county having a population in excess of 750,000, with the consent of the district attorney.

33

- (F) A city prosecutor in any city having a full-time city prosecutor or, with the consent of the district attorney, by a city attorney in any city and county.
- (G) The Director of the Office of Health Information Integrity may recommend that any person described in subparagraphs (A) to (F), inclusive, bring a civil action under this section.

34

## Civil Code 56.36(e) (cont.)

- (2) If the action is brought by the Attorney General, one-half of the penalty collected shall be paid to the treasurer of the county in which the judgment was entered, and one-half to the General Fund. If the action is brought by a district attorney or county counsel, the penalty collected shall be paid to the treasurer of the county in which the judgment was entered. Except as provided in paragraph (3), if the action is brought by a city attorney or city prosecutor, one-half of the penalty collected shall be paid to the treasurer of the city in which the judgment was entered and one-half to the treasurer of the county in which the judgment was entered.
- (3) If the action is brought by a city attorney of a city and county, the entire amount of the penalty collected shall be paid to the treasurer of the city and county in which the judgment was entered.

35

## Questions?

36